REMARKS

The above amendments and following remarks are submitted within the priority period under 37 C.F.R. 1.116 in response to the final official action of the Examiner mailed August 31, 2004. Having addressed all objections and grounds of rejection claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

The Examiner has rejected claims 1-20, being all pending claims, under 35 U.S.C. 112, first paragraph. This ground of rejection is respectfully traversed as based upon clearly erroneous findings of fact. In support of his rejection, the Examiner states at paragraph 8 of his rejection:

> Independent claims 1, 6, 11 and 16 cite limitations whereby a user is validated at an Internet terminal through the entry of a user identifier and password, and wherein the Internet terminal contains a site-specific <u>terminal identifier</u>. (Emphasis added)

The Examiner continues at paragraph 38, stating:

> ....and also the fact that the term '<u>terminal identifier</u>' is not used in the specification, the claims are not enabled by the disclosure to a sufficient degree to allow an ordinary artisan to make and use the invention. (Emphasis added)

It seems apparent that the Examiner has clearly erroneously found that the pending claims utilize the term, "terminal identifier". This is incorrect. Applicants have previously utilized this term to distinguish a "site-specific user-id" from a "user-specific

10

user-id" to make their arguments, perhaps unwisely. However, the term is not found in the pending claims.

Secondly, at paragraph 38, the Examiner also states:

> ....the extent of the detailed disclosure within the specification that is concerned with the claimed security system is limited to the summary of the invention, pages 7-9, and the discussion of Figure 10, pages 33-34...

This statement is also clearly erroneous. As has been previously explained in great detail, the site-specific identifier is in general handled by the system as if it were a specific user identifier. Therefore, the basic discussion of the handling of security profiles of Fig. 2 and corresponding description at pages 14-16, for example, is directly pertinent. Furthermore, Figs. 11-14 are completely directed to the specifics of the claimed invention.

Thirdly, the Examiner states in paragraph 8 of his rejection:

> Figure 13 illustrates a number of <u>software method</u> calls, <u>disclosing only the names of the methods</u> and arguments passed. (Emphasis added)

Continuing in paragraph 8, he states:

> Figure 14 illustrates a number of 'messages' and descriptions.

These findings are directly on point. The "software methods" referenced are found in the prior art as cited by the Examiner, cited by Applicants, commercially available from the Assignee of the subject invention, and part of the

11

record of this prosecution. Therefore, even though they are only named, this is deemed sufficient to enable one of skill in the art to make and use the claimed invention.

That which is unique to the preferred mode of the present invention is the order in which these "software methods" are called, the arguments presented to these preexisting "software methods", and the unique sequence of message associated with the process of creating the site-specific user-id. As admitted by the Examiner, these are disclosed in detail. After a site-specific user-id has been created in this fashion, it is handled as if it were a user-specific user-id. The site-specific user-id is maintained in accordance with Figs. 11-12, along with accompanying description found at pages 35-37.

In accordance with paragraph of the Examiner's final rejection, page 34 of the specification has been amended as suggested by the Examiner. No new matter has been added.

Claims 1 and 2 have been rejected under 35 U.S.C. 112, second paragraph. In response thereto, Applicants have herewith amended claims 1 and 2.

Claims 1-4, 6-8, 11-14, and 16-18 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison:) in view of the article entitled "Access Control in

12

Federated Systems" by De Capitani di Vimercati et al (hereinafter

referred to as "De Capitani di Vimercati) in view of U.S. Patent

No. 6,282,175, issued to Steele et al (hereinafter referred to as

"Steele"). This ground of rejection is respectfully traversed

for failure of the Examiner to meet his burden of showing the

three elements required by MPEP 2143.

With regard to motivation to make the alleged combination of

De Capitani di Vimercati with Garrison in rejecting claim 1, the

Examiner admits:

> Garrison does not explicitly teach a data processing
> environment wherein the user accesses the database by
> transferring a second user identifier which uniquely
> identifies a particular site without transfer of said
> user identifier via said publicly accessible digital
> data communication network.

In making his motivational argument, the Examiner ignores the

actual teaching of De Capitani di Vimercati and simply suggests

the motivation to combine because the two references exist and

are concerned with related fields.

Actually, one of ordinary skill in the art reading De

Capitani di Vimercati would **not** form the alleged combination,

because the reference says that one should not. The Examiner's

citation of the reference states:

> However, this approach [i.e., not transferring the
> user-specific identifier] would require access
> authorizations to be specified only with respect to
> remote identities. The approach of always requiring
> explicit connection to the federation is preferable in
> general, since it allows authorizations on federated
> data to be specified against identifiers established

13

and managed by the federation administrator. ....
Let us therefore assume that each user needs to
identify himself at the federation.

Thus, instead of motivating the alleged combination, De Capitani
di Vimercati actually teaches away from it.

In response to Applicants' previous argument of lack of
motivation to make the alleged combination, the Examiner has
cited MPEP 2123 which discusses whether non-preferred embodiments
constitute prior art.   This citation completely misses the point.
Motivation of the alleged combination of Garrison and De Capitani
di Vimercati is absent because De Capitani di Vimercati teaches
away from the alleged combination not because of a lack of prior
art status,

The Examiner does not even allege a reasonable likelihood of
success of the allege combination, much less meet the burden of
MPEP 2143.

With regard to the alleged combination of Steele with
Garrison and De Capitani di Vimercati, the Examiner admits:

> Neither Garrison nor De Capitani di Vimercati et al.
> explicitly teaches a data processing environment
> wherein said service request is honored by executing a
> sequence of command language scripts having an
> associated security profile.

In alleging motivation, the Examiner states:

> It would have been obvious to one of ordinary skill in
> the art at the time of the invention to satisfy service
> requests through the execution of command language
> scripts having an associated security profile, since
> (sic) this allows a system to provide pre-defined data
> request that can be accessed by a client terminal at

14

> the touch of a button, rather than requiring said
> client terminal to manually format such a request (see
> Steele et al., col. 7, lines 33-56). (emphasis added)

Though this conclusion is not supported by the Examiner's citation, even if it were, it would not provide the alleged motivation, because there is no showing that Garrison requires the "client terminal to manually format such a request". In fact, Garrison actually states at column 7, lines 30-32:

> In the preferred embodiment, the request for data is a
> predetermined data word (i.e., a code word) known to
> the server 17a.

Thus, the attempted showing of motivation to add Steele to the alleged combination is based upon clearly erroneous findings of fact and incorrect application of controlling law.

Again, the Examiner does not even attempt to meet his burden under MPEP 2143 of showing reasonable likelihood of success.

Having not shown motivation or reasonable likelihood of success, the Examiner fails to show the third element of MPEP 2143, that all claimed limitations are found within the alleged combination. Claim 1, as amended, requires an "administration module" and "a security profile maintained by said administration module and stored in association with said sequence of command language script". The alleged combination does not have either of these elements.

Therefore, the rejection of claim 1, and all claims depending therefrom, is respectfully traversed for failure of the

15

Examiner to present a *prima facie* case of obviousness as required by MPEP 2143.

In his rejection of claim 6, the Examiner again totally ignores his obligation to show reasonable likelihood of success of the alleged three reference combination. In addition, the Examiner has failed to show motivation for the alleged combination for the reasons discussed in detail above. Furthermore, claim 6 has three separate and distinct limitations, of which the alleged combination lacks two. Claim 6 is limited by: 1) "a data base management system .... which executes a sequence of command language script to honor said service request"; and 2) "a security profile .... corresponding to said sequence of command language script whereby said data base management system executes said sequence of command language script to provide access to a particular secure portion of said data base". The alleged combination does not have either of these two elements.

Therefore, the rejection of claim 6, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

In his rejection of claim 11, the Examiner again totally ignores his obligation to show reasonable likelihood of success of the alleged three reference combination. In addition, the

16

Examiner has failed to show motivation for the alleged
combination for the reasons discussed in detail above.
Furthermore, independent method claim 11 has six separate and
distinct steps, of which the alleged combination lacks steps b
and d. Claim 11 is limited by: b)"transmitting a service request
requiring execution of a sequence of command language statements
to provide secure access to said data base ....”; and d)
"determining a security profile corresponding to said sequence of
command language statements utilizing an administration module".
The alleged combination does not have either of these two method
steps.

Therefore, the rejection of claim 11, and all claims
depending therefrom, is respectfully traversed for failure of the
Examiner to make a *prima facie* case of obviousness as specified
by MPEP 2143.

In his rejection of claim 16, the Examiner again totally
ignores his obligation to show reasonable likelihood of success
of the alleged three reference combination. In addition, the
Examiner has failed to show motivation for the alleged
combination for the reasons discussed in detail above.
Furthermore, claim 16 has three separate and distinct
limitations, of which the alleged combination lacks two. Claim
16 is limited by: 1)"offering means .... for offering data
processing services involving access to said data base in

17

response to said service request by executing a sequence of command language script"; and 2) "preventing means .... for preventing .... unless said site corresponds to a security profile associated with said sequence of command language script and maintained by an administration module". The alleged combination does not have either of these two elements.

Therefore, the rejection of claim 16, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

In his rejection of claim 2, the Examiner states:

> Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

This finding is clearly erroneous. The Examiner's citation says nothing of a "security profile" and certainly says nothing of how any security codes are "generated". The rejection of claim 2 and any claim depending therefrom is respectfully traversed as based upon clearly erroneous findings of fact.

Claims 3, 8, 12, 13, and 18 require a particular service request to include a site-specific user-id. Contrary to the Examiner's clearly erroneous findings of fact, Garrison separates client authorization and data retrieval into two separate functions (see for example Fig. 4A). The request for data

18

(element 126 of Fig. 4A) is not transmitted by the client until password verification (element 117 of Fig. 4A).

In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to impart greater granularity of security profiling. A given user may be authorized to make certain service request but not others. In general, most users will not be authorized to make all service requests. The rejection of claims 2, 8, 12, 13, and 18 is respectfully traversed as based upon clearly erroneous findings of fact.

Claims 4, 14, and 17 depend from claims 3, 13, and 16, respectfully, and further limit the publicly accessible digital data communication network. As such they each present new and unique combinations not found in the prior art of record. The rejection of claims 4, 14, and 17 is respectfully traversed.

Claim 7 depends from claim 6 and is further limited by "wherein said terminal accesses said data base by transferring said service request to said data base management system". The Examiner cites Garrison column 6, line 60, through column 7, lines 32, and column 7, line 50, through column 8, line 37. Neither of these citations has even mentions a "service request". Though the term, "service request", has standard usage in the art, a working definition is provided by Applicants at page 25, lines 11-16, as:

19

The service request itself is utilized by Cool ICE
service handler 156 to retrieve a previously stored
sequence of data base management system command
statements from repository 166. Thus, in the general
case, a single service request will result in the
execution of a number of ordered data base management
system commands. The exact sequence of these commands
is defined by the service request developer as
explained in more detail below.

The rejection of claim 7 is respectfully traversed as based upon

clearly erroneous findings of fact.

Claims 5, 9, 10, 15, 19, and 20 have been rejected under 35

U.S.C. 103(a) as being unpatentable over Garrison in view of De

Capitani di Vimercati in view of Steele and further in view of

"UNISYS CSG MarketPlace - The Mapper System" (hereinafter

referred to as "UNISYS"). This ground of rejection is

respectfully traversed for failure of the Examiner to present a

prima facie case of obviousness as required by MPEP 2143.

None of Garrison, De Capitani di Vimercati, nor Steele

mentions a "data base management system". Therefore, it makes no

sense to allege that one of skill in the art would be motivated

to combine the teachings of UNISYS to provide a particular data

base management system. Lacking motivation, it is extremely

apparent that there is no reasonable likelihood of success of the

alleged combination without the teachings of Applicants. The

rejection of claims 5, 9, 10, 15, 19, and 20 is respectfully

traversed for failure of the Examiner to make a prima facie case

of obviousness.

20

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.
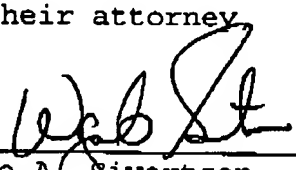
Please charge any deficiencies or credit any overpayment to Deposit Account No. 14-0620.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date October 28, 2004

Wayne A. Sivertson
Reg. No. 25,645
Suite 401
       Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota
       55413
(612) 331-1464

21